The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/11/2012

SUBJECT:

Multiple Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS12-078)

OVERVIEW:

Two vulnerabilities have been discovered in Microsoft Windows that could allow for remote code execution. These vulnerabilities are due to improper validation of input by Windows kernel-mode drivers. Exploitation of these vulnerabilities could result in the execution of arbitrary code with administrative privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows server 2012
- Windows RT

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users:High

DESCRIPTION:
Two vulnerabilities have been identified in Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for code execution. The details of the vulnerabilities are as follows:

_OpenType Font Parsing Vulnerability (_CVE-2012-2556)_:_
This vulnerability is triggered when the OpenType Font (OTF) driver does not properly handle objects in memory.

TrueType Font Parsing Vulnerability (CVE-2012-4786)
This remote execution vulnerability is caused when Windows TrueType font parsing improperly handles objects in memory.

These vulnerabilities can be exploited by multiple methods:

- Web browsing attack scenario – an attacker could create a webpage that is used to exploit this vulnerability. For successful exploitation, a user must visit the webpage, or click on a link in an email.
- Email attachment attack scenario – a specially crafted file that takes advantage of this vulnerability can be sent as an email attachment. In order for exploitation to be successful, the user must open the attachment.
- File sharing attack scenario - a specially crafted file that takes advantage of this vulnerability is stored on a network-shared drive. For successful exploitation, a user must open the document file.

Successful exploitation of any of these vulnerabilities could result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

- Remind users not to download or open files from un-trusted websites.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms12-078

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2556
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4786

Security Focus:
http://www.securityfocus.com/bid/56841
http://www.securityfocus.com/bid/56842